AMENDMENT TO THE CLAIMS

1. (Currently Amended) A method of evaluating fraud risk of an electronic commerce transaction, the method comprising the computer-implemented steps of:

receiving transaction data that defines the electronic commerce transaction;

determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein each of the plurality of tests determines whether the transaction data appears to represent a genuine transaction based on specified criteria;

determining a second fraud risk score value associated with the electronic commerce transaction based on a comparison of the transaction data to historical transaction data;

combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value; and

blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the electronic commerce transaction;

wherein receiving transaction data comprises the steps of receiving transaction data that defines the electronic commerce transaction for a particular Internet identity, and wherein determining a second fraud risk score value comprises the steps of determining a second fraud risk score value associated with the electronic commerce transaction based on a comparison of the transaction data to historical transaction data for other electronic commerce transactions pertaining to the same Internet identity;

wherein the particular Internet identity comprises a first hash value of an email address of a prospective purchaser carried in combination with a second hash value of a card bank identification number of the prospective purchaser[[.]]; and

wherein the step of blending the model score value comprises the steps of:

determining in which fraud risk zone, of two or more fraud risk zones, the boundaries of which are determined by the one or more merchant-specific

threshold values, the model score value belongs; and

applying a policy corresponding to the determined fraud risk zone, wherein the policy dictates a magnitude and an allowable direction of influence applied by a heuristic model and a statistical model.

2. (Canceled)

3. (Canceled)

4. (Previously Presented) A method as recited in Claim 1, wherein the particular Internet identity comprises a first hash value of an email address of a prospective purchaser carried in combination with a second hash value of a card bank identification number of the prospective purchaser and with a third hash value based on a shipping address of the prospective purchaser.

5. (Previously Presented) A method as recited in Claim 1, wherein the particular Internet identity comprises a first hash value of an prospective purchaser's host IP address, in combination with a second hash value of an email address of a prospective purchaser carried, in combination with a third hash value of a card bank identification number of the prospective purchaser and a fourth hash value based on a shipping address of the prospective purchaser.

6. (Previously Presented) A method as recited in Claim 1, wherein the particular Internet identity comprises a first hash value of a prospective purchaser's hardware device ID value, in combination with a second hash value of either the email address or user ID of the prospective purchaser, in combination with a third hash value of a card bank identification number of the prospective purchaser and with a fourth hash value based on a shipping address of the prospective purchaser.

7. (Previously presented) A method as recited in Claim 1, wherein the step of determining the second fraud risk score value comprises the steps of:

retrieving one or more records of historic transaction data pertaining to past transactions associated with the transaction data;

when one of the records of historic transaction data is found to contain a fraud list tag, discontinuing further retrieval of such records;

determining the second fraud risk score value associated with the electronic commerce transaction based on only the retrieved records of historical transaction data in comparison to the transaction data.

8. (Previously presented) A method as recited in Claim 1, wherein the step of determining the second fraud risk score value comprises the steps of:

retrieving one or more records of historic transaction data pertaining to past electronic commerce transactions associated with the transaction data;

when a specified amount of the records of historic transaction data is retrieved and further records of historic transaction data remain to be retrieved, discontinuing further retrieval of such records;

determining the second fraud risk score value associated with the electronic commerce transaction based on only the retrieved records of historical transaction data in comparison to the transaction data.

9. (Previously presented) The method as recited in Claim 1, wherein the step of blending the model score value comprises the steps of blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the electronic commerce transaction and one or more return code values that signal specified risk issues that have been detected with respect to the transaction.

10. (Previously presented) The method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein one of the plurality of tests determines whether an Internet identity in the transaction data is found in a list of parties to known past fraudulent transactions.

11. (Previously presented) The method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein one of the plurality of tests determines whether an Internet identity in the transaction data is found in a list of trusted parties.

12. (Previously presented) A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein one of the plurality of tests comprises the steps of:
receiving the text value;
for each bi-gram in the text value, retrieving from a table of bi-gram probability values a probability value that represents a probability that the bi-gram is found in a genuine text value;
generating a penalty value when the retrieved probability values indicate that the text value comprises a combination of bi-grams that are not likely to represent a genuine text value.

13. (Previously presented) A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, by the steps of:
receiving the name value;

for each bi-gram in the text value, retrieving from a table of bi-gram probability values a probability value that represents a probability that the bi-gram is found in a genuine name value, wherein the table of bi-gram probability values is created based on an actual frequency of occurrences of bi-grams in a large sample of genuine names;

generating a penalty value when the retrieved probability values indicate that the text value comprises a combination of bi-grams that are not likely to represent a genuine name value.

14. (Previously presented) A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein one of the plurality of tests automatically determines whether a city value in the transaction data is within an area code value of the transaction data, by the steps of:

receiving the city value and the area code value as part of the transaction data;

determining a latitude value and a longitude value that represent a position of a city identified in the city value;

determining a range of latitude values and a range of longitude values associated with an area code identified in the area code value;

based on the latitude value, the longitude value, the range of latitude values, and the range of longitude values, determining whether the city identified in the city value is within the area code identified in the area code value;

applying a penalty to the electronic commerce transaction when the city identified in the city value is not within the area code identified in the area code value.

15. (Previously presented) A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein one of the plurality of tests automatically determines whether a city value in the transaction data is within an email domain of the transaction data, by the steps of:

receiving the city value and an email address value as part of transaction data;

determining a latitude value and a longitude value that represent a position of a city identified in the city value;

determining a range of latitude values and a range of longitude values associated with an email domain portion of the email address value;

based on the latitude value, longitude value, the range of latitude values, and the range of longitude values, determining whether the city identified in the city value is within the email domain indicated in the email address value;

applying a penalty to the electronic commerce transaction when the city identified in the city value is not within the area code identified in the area code value.

16. (Previously Presented) A method as recited in Claim 15, further comprising the steps of creating and storing an email domain location table comprising a plurality of records that associate email domain values with city values associated with shipping addresses of past non-fraudulent transactions.

17. (Previously Presented) The method as recited in Claim 16, wherein determining whether the city identified in the city value is within the email domain comprises the steps of determining whether the city value is for a city that is outside the email domain as indicated by the records in the email domain location table.

18. (Previously presented) A method as recited in Claim 1, wherein determining the first fraud risk score value comprises the steps of determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein one of the plurality of tests automatically determines whether a country value in the transaction data is proximate to a bank referenced in a bank identification number of a credit card number in the transaction data, by the steps of:

receiving the country value and a bank identification number of a credit card number as part of the transaction data;

determining a relative distance between a country identified in the country value and a bank associated with the bank identification number;

based on the relative distance between the country and the bank, determining whether the country is greater than a specified relative distance from the bank;

applying a penalty to the electronic commerce transaction when the country is greater than the specified relative distance from the bank.

19. (Previously presented) A method as recited in Claim 18, further comprising the steps of creating and storing a bank location table comprising a plurality of records, wherein each record associates a bank identification number with a country value representing a country in which a headquarters of the bank is located.

20. (Previously presented) A method as recited in Claim 19, further comprising the steps of creating and storing a bank location table comprising a plurality of records that associate bank identification numbers with country values associated with shipping addresses of past non-fraudulent transactions.

21. (Previously presented) The method as recited in Claim 20, wherein determining whether the country identified in the country value is greater than the specified relative distance from the bank comprises the steps of determining whether the country value is for a country that is greater than the specified relative distance from the bank as indicated by the records in the bank domain location table.

22. (Previously Presented) A method of determining evaluating fraud risk of an electronic commerce transaction, the method comprising the computer-implemented steps of:

receiving transaction data that defines the electronic commerce transaction;

determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein one of the plurality of tests includes at least:

receiving the name value;

for each bi-gram in the text value, retrieving from a table of bi-gram probability values a probability value that represents a probability that the bi-gram is found in a genuine name value, wherein the table of bi-gram probability values is created based on an actual frequency of occurrences of bi-grams in a large sample of genuine names;

generating a penalty value when the retrieved probability values indicate that the text value comprises a combination of bi-grams that are not likely to represent a genuine name value; and

wherein receiving transaction data comprises the steps of receiving transaction data that defines the electronic commerce transaction for a particular Internet identity, and wherein determining a second fraud risk score value comprises the steps of determining a second fraud risk score value associated with the electronic commerce transaction based on a comparison of the transaction data to historical transaction data for other electronic commerce transactions pertaining to the same Internet identity;

wherein the particular Internet identity comprises a first hash value of an email address of a prospective purchaser carried in combination with a second hash value of a card bank identification number of the prospective purchaser.

23. (Canceled)

24. (Currently Amended) A computer-readable medium carrying one or more sequences of instructions for evaluating fraud risk of an electronic commerce transaction, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving transaction information that defines the electronic commerce transaction;

determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein each of the plurality of tests determines whether the transaction data appears to represent a genuine transaction based on specified criteria;

determining a second fraud risk score value associated with the electronic transaction based on a comparison of the transaction information to historical transaction information;

combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value; and

blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the electronic commerce transaction;

wherein receiving transaction data comprises the steps of receiving transaction data that defines the electronic commerce transaction for a particular Internet identity, and wherein determining a second fraud risk score value comprises the steps of determining a second fraud risk score value associated with the electronic commerce transaction based on a comparison of the transaction data to historical transaction data for other electronic commerce transactions pertaining to the same Internet identity;

wherein the particular Internet identity comprises a first hash value of an email address of a prospective purchaser carried in combination with a second hash value of a card bank identification number of the prospective purchaser[[.]]; and

wherein the step of blending the model score value comprises the steps of:

determining in which fraud risk zone, of two or more fraud risk zones, the boundaries of which are determined by the one or more merchant-specific

threshold values, the model score value belongs; and

applying a policy corresponding to the determined fraud risk zone, wherein the policy dictates a magnitude and an allowable direction of influence applied by a heuristic model and a statistical model.

25. (Currently Amended) An apparatus for evaluating fraud risk of an electronic commerce transaction, the apparatus comprising:

means for receiving transaction data that defines the electronic commerce transaction;

means for determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein each of the plurality of tests determines whether the transaction data appears to represent a genuine transaction based on specified criteria;

means for determining a second fraud risk score value associated with the electronic commerce transaction based on a comparison of the transaction data to historical transaction data;

means for combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value; and

means for blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the electronic commerce transaction;

wherein the means for receiving transaction data comprises means for receiving transaction data that defines the electronic commerce transaction for a particular Internet identity, and wherein the means for determining a second fraud risk score value comprises means for determining a second fraud risk score value associated with the electronic commerce transaction based on a comparison of the transaction data to historical transaction data for other electronic commerce transactions pertaining to the same Internet identity;

wherein the particular Internet identity comprises a first hash value of an email address of a prospective purchaser carried in combination with a second hash value of a card bank identification number of the prospective purchaser[[.]]; and

wherein the means for blending the model score value comprises:

means for determining in which fraud risk zone, of two or more fraud risk zones, the boundaries of which are determined by the one or more merchant-specific threshold values, the model score value belongs; and

means for applying a policy corresponding to the determined fraud risk zone, wherein the policy dictates a magnitude and an allowable direction of influence applied by a heuristic model and a statistical model.

26. (Currently Amended) An apparatus for evaluating fraud risk of an electronic commerce transaction, comprising:

a processor;

a computer readable medium having one or more sequences of instructions stored thereon which, when executed by the processor, cause the processor to carry out the steps of:

receiving transaction data that defines the electronic commerce transaction;

determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction data, wherein each of the plurality of tests determines whether the transaction data appears to represent a genuine transaction based on specified criteria;

determining a second fraud risk score value associated with the electronic commerce transaction based on a comparison of the transaction data to historical transaction data;

combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value; and

blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the electronic commerce transaction;

wherein receiving transaction data comprises the steps of receiving transaction data that defines the electronic commerce transaction for a particular Internet identity, and wherein determining a second fraud risk score value comprises the steps of determining a second fraud risk score value associated with the electronic commerce transaction based on a

comparison of the transaction data to historical transaction data for other electronic commerce transactions pertaining to the same Internet identity;

wherein the particular Internet identity comprises a first hash value of an email address of a prospective purchaser carried in combination with a second hash value of a card bank identification number of the prospective purchaser[[.]]; and

wherein the step of blending the model score value comprises the steps of:

determining in which fraud risk zone, of two or more fraud risk zones, the boundaries of which are determined by the one or more merchant-specific threshold values, the model score value belongs; and

applying a policy corresponding to the determined fraud risk zone, wherein the policy dictates a magnitude and an allowable direction of influence applied by a heuristic model and a statistical model.

27. (Canceled)

28. (Previously presented) A method as recited in claim 1, wherein:

receiving the transaction data is performed by a first apparatus that is linked to a second apparatus by a network; and

blending the model score value is performed by the second apparatus.

29. (Canceled)

30. (Currently Amended) A computer-readable medium carrying one or more sequences of instructions for evaluating fraud risk of an electronic commerce transaction, when executed by one or more processors, the computer readable medium comprising:

memory carrying one or more instructions that cause the one or more processors to carry out the step of receiving transaction information that defines the electronic commerce transaction;

memory carrying one or more instructions that cause the one or more processors to carry out the step of determining a first fraud risk score value associated with the electronic commerce transaction based on applying a plurality of tests to the transaction information, wherein each of the plurality of tests determines whether the transaction information appears to represent a genuine transaction based on specified criteria;

memory carrying instructions one or more instructions that cause the one or more processors to carry out the step of determining a second fraud risk score value associated with the electronic transaction based on a comparison of the transaction information to historical transaction information;

memory carrying one or more instructions that cause the one or more processors to carry out the step of combining the first fraud risk score value and the second fraud risk score value using a statistical model to result in creating a model score value; and

memory carrying one or more instructions that cause the one or more processors to carry out the step of blending the model score value with one or more merchant-specific threshold values to result in creating and storing a final fraud risk score value for the electronic commerce transaction;

wherein the instructions that cause receiving transaction data comprises instructions that cause receiving transaction data that defines the electronic commerce transaction for a particular Internet identity, and wherein the instructions that cause determining a second fraud risk score value comprise instructions that cause determining a second fraud risk score value associated with the electronic commerce transaction based on a comparison of the transaction data to historical transaction data for other electronic commerce transactions pertaining to the same

Internet identity;

wherein the particular Internet identity comprises a first hash value of an email address of a prospective purchaser carried in combination with a second hash value of a card bank identification number of the prospective purchaser[[.]]; and

wherein the instructions that cause blending the model score value comprise:

instructions that cause determining in which fraud risk zone, of two or more fraud risk zones, the boundaries of which are determined by the one or more merchant-specific threshold values, the model score value belongs; and

instructions that cause applying a policy corresponding to the determined fraud risk zone, wherein the policy dictates a magnitude and an allowable direction of influence applied by a heuristic model and a statistical model.